REMARKS/ARGUMENTS

In response to the Office Action of December 30, 2005, please consider the following remarks.

In the Office Action mailed December 30, 2005, claims 2-6, 8-26, and 28 were rejected under 35 U.S.C. § 102(e), as being allegedly anticipated by US Patent 6,233,565 (hereinafter, "Lewis et al."). Claims 1 and 27 was rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Lewis in view of US Patent 6,785,810 (hereinafter "Lirov et al."). Claim 7 was rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Lewis in view of US Patent 6,598,167 (hereinafter "Devine et al.).

Claims 1-3, 5, 7-24, 26-31 are currently pending in the application. Claims 29-31 are new. Reconsideration of the instant application by the Examiner in view of the remarks below is respectfully requested.

The Prior Art

Lewis et al. discloses a secure transport for registration and password authentication. As Lewis et al. describe in the Abstract, a transaction authentication system includes authentication, wherein the client authentication module and the server authentication modules communicate via the internet connection and are authenticated to each other. Thus, Lewis et al. describe transactions between client and server. All references to encryption are performed either by the client or the server. No encryption appliance is used between the client and server to perform encryption on (only) the most sensitive parts of the transaction.

Notably, Lewis et al. use a hardwired protocol, which is not configurable regarding what is encrypted and not encrypted. Thus, Lewis et al. cannot dynamically determine what data is sensitive data. For example, Lewis et al., at col. 17, lines 15-30, describe a transaction wherein a server is informed of the type of transaction so that the server knows what fields will be included in the transaction. This is fundamentally different than receiving a sequence of packets and determining whether any sensitive data is in the sequence of packets, and cryptographically transforming the sensitive data if any is found. Therefore, Lewis et al. do not describe a system that is capable of encrypting/decrypting specific elements of a transaction based upon an analysis of the individual transaction, but rather a system that receives transactions in a pre-defined format.

Similarly, Lirov et al. do not say how a determination is made to identify sensitive data. Presumably, data is sensitive if the data is entered into a field that is sensitive. No dynamic or other description of an identification procedure is disclosed or implied.

Devine is used to reject only dependent claim, and is therefore not described in any detail herein. However, it is noted that Devine also do not describe the use of pattern matching to identify sensitive data.

The Prior Art Distinguished

Claim 1 includes the language "applying a user-defined pattern matching expression to identify sensitive data within the at least one electronic transaction query[.]" To anticipate a claim, a prior art reference must teach each and every element of a claim. Lewis et al. do not apply a user-defined pattern matching expression to identify sensitive data. Rather, the transactions of Lewis et al. are in a predefined format. Moreover, Lewis et al. would not be motivated to apply a user-defined pattern matching expression to identify sensitive data because the sensitive data is statically pre-determined by virtue of the data being entered in a field that is sensitive. It may be noted that Lirov et al. do not make up for this deficiency. Accordingly, Claim 1 is allowable over the prior art.

Claim 2 includes the language "applying a pattern matching expression to identify sensitive data elements inside the electronic request[.]" For reasons similar to those described with reference to claim 1, claim 2 is allowable over the prior art. Claims

3, 5, and 7-13, which depend from Claim 2, are allowable at least for depending for an allowable base claim, and potentially for additional reasons.

For example, claim 3 includes the language "determining that the at least one electronic request includes sensitive data." Lewis et al. do not make any effort to determine whether an electronic request includes sensitive data. Either the transaction includes a field that is sensitive, or it does not. No determination is necessary. Therefore, Lewis et al. would not be motivated to determine whether a request include sensitive data, as recited in claim 3. Lirov et al. do not make up for this deficiency.

As another example, claim 5 includes the language "determining that sensitive data in the electronic request includes at least one user password[.]" Lewis et al. do not determine whether the sensitive data includes a password. Either the request has a field with a password, or the request does not. No determination is necessary. Therefore, Lewis et al. would not be motivated to determine whether a request includes a password, as is recited in claim 5. Lirov et al. do not make up for this deficiency.

Claim 14 includes the language "dynamically determining that the at least one electronic request includes sensitive data [and] encrypting the sensitive data[.]" Lewis et al. do not dynamically determine whether a transaction includes sensitive data. In Lewis et al. a transaction that includes sensitive data is in a pre-defined, static format. No dynamic determination is disclosed or implied. Lirov et al. do not make up for this deficiency. Claims 15-16, which depend from Claim 14, are allowable at least for depending for an allowable base claim, and potentially for additional reasons. Claim 17 is allowable for reasons similar to those described with reference to claim 15.

Claim 18 includes the language "the at least one processing device identifies, using regular expressions, sensitive data inside the electronic request[.]" Lewis et al. and Lirov et al. do not disclose or imply using regular expressions to identify sensitive data. Claims 19-22, which depend from Claim 18, are allowable at least for depending for an allowable base claim, and potentially for additional reasons.

Claim 23 includes the language "at least one processing device... to evaluate at least one received electronic request in a first protocol format, wherein the at least one processing device; determines when the at least one received electronic request includes sensitive data; encrypts the sensitive data; reforms the electronic request, including the encrypted sensitive data, in the first protocol format, and transfers the reformed electronic request among at least one component of the at least one server system." Lewis et al. and Lirov et al. do not describe or suggest encrypting sensitive data received in a first protocol format and reforming a request, including the encrypted sensitive data, ***in the same [first] protocol format***. Indeed, if the transaction format for, say, a credit card, was alphanumeric, encrypting the credit card information and passing it along in the same format would potentially break the Lewis et al. and Lirov et al. systems (since the servers would expect to receive an alphanumeric value rather than a cryptographically transformed data unit). Claim 24, which depends from Claim 23, is allowable at least for depending for an allowable base claim. In addition, claim 24 includes the language "evaluates at least one request for the encrypted sensitive data... decrypts the encrypted sensitive data[.]" Thus, claim 24 is allowable at least for reasons similar to those described with reference to claim 17.

Claim 26 and 27 are allowable for reasons similar to those described above with reference to claim 14. In addition, the applicants respectfully disagree that Lirov et al. expressly discloses reading a configuration file at col. 8, line 65 through col. 9, line 10, as asserted by the Examiner at page 12 of the Office Action. Claim 28 is allowable for reasons similar to those described with reference to claim 18. Claim 29 is allowable for reasons similar to those described with reference to claims 1 and/or 23.

Conclusion

In view of the foregoing, the Applicants respectfully submit that the pending claims are allowable. The Applicants respectfully request the Examiner withdraw the rejections of all claims. The Applicants respectfully request that a timely Notice of Allowance be issued in this case.

Should the Examiner have any questions or comments, he is encouraged to call the undersigned at (650) 838-4305 so that any outstanding issues can be expeditiously resolved.

Respectfully submitted,
Perkins Coie LLP

Date: May 30, 2006

William F. Ahmann
Reg. No. 52,548

Correspondence Address:
Customer No. 22918
Perkins Coie LLP
P.O. Box 2168
Menlo Park, California 94026
(650) 838-4300